IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

SHACARAH SCOTT and JOSHUA TUCKER, individually and on behalf of all others similarly situated,	)	
Plaintiffs,	)	Case No. _____
v.	)	
SYNCREON NORTH AMERICA, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

COME NOW Plaintiffs, Shacarah Scott and Joshua Tucker, on behalf of themselves and all others similarly situated, and for their cause of action against Defendant, state as follows:

Plaintiffs, individually and on behalf of others similarly situated, bring this Class Action Complaint against Defendant to stop Defendant's capture, collection, use, and storage of individuals' biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. ("BIPA"), and the common law, and to obtain redress for persons injured by its conduct. Plaintiffs allege the following based on personal knowledge and experiences, and as to all other matters upon information and belief, including an investigation conducted by their attorneys.

PARTIES

1. At all relevant times, Plaintiffs, SHACARAH SCOTT and JOSHUA TUCKER (hereafter, "Plaintiffs"), have been residents and citizens of the State of Illinois, residing in Madison County, Illinois, and worked for Defendant in Madison County, Illinois.

2. Defendant, SYNCREON NORTH AMERICA, INC. (hereafter "SNA"), is a foreign corporation registered and licensed to do business in Illinois, and conducting a significant business in Madison County, Illinois, with its principal place of business in Auburn Hills, Michigan.

3. At all relevant times, SNA employed in excess of 100 employees at its Madison County, Illinois, facility and was thus an employer and private entity covered as defined under BIPA.

JURISDICTION AND VENUE

4. This Court has Diversity Jurisdiction under 28 U.S.C. § 1332(d) because: (i) at least one member of the putative class is a citizen of a state different from Defendant; (ii) the amount in controversy exceeds $5,000,000 exclusive of interest and costs; and (iii) none of the exceptions under that subsection apply to this action.

5. This Court has personal jurisdiction over Defendant because Defendant transacts and/or transacted business in Illinois during the relevant time period and a substantial part of the events giving rise to Plaintiffs' claims arise out of Defendant's unlawful in-state actions, as Defendant captured, collected, stored, and used Plaintiffs' biometrics in this State.

6. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because asubstantial part of the events giving rise to Plaintiffs' claims occurred in this District, as Defendant captured, collected, stored, and used Plaintiffs' biometrics at one of its facilities located in this District.

INTRODUCTION

7. Defendant implemented, without notice to its employees or the consent of its employees, an invasive timekeeping program of capturing, collecting, storing, and using Plaintiffs' and other SNA employees' fingerprints. Defendant uses employees' fingerprint scans to identify

such employees for timekeeping and payroll purposes. In so doing, Defendant has repeatedly violated BIPA.

8. The nature of the substantive privacy interests at issue here has been recognized by the Illinois Legislature pursuant to BIPA. Moreover, the Federal Trade Commission and numerous privacy experts have also recognized the substantive privacy interests at issue as well as the resultant injury when those interest are violated. Furthermore, expert studies show that such injuries can be quantified in dollars and cents. For those reasons and others, courts in this District and elsewhere have recognized the substantive privacy rights given to persons in their biometric information under BIPA.

9. Plaintiffs bring this action for damages and other remedies resulting from the actions of SNA in capturing, collecting, storing, using, and disseminating his biometrics, and those of hundreds or thousands of Defendant's workers throughout the state of Illinois, without informed written consent, and without informing them through a publicly available policy of how and when the subject biometrics would be stored or disposed of, in direct violation of the Illinois BIPA. To the extent SNA is still retaining Plaintiffs' biometrics, such retention is unlawful. Plaintiffs would not have provided their biometric data to SNA had they known the same would remain with SNA for an indefinite period or subject to unauthorized disclosure.

10. On behalf of themselves and the proposed Class defined below, Plaintiffs seek an injunction requiring SNA to comply with BIPA, as well as an award of statutory damages to the Class members and common law monetary damages to be determined at trial, together with costs and reasonable attorneys' fees.

FACTUAL BACKGROUND

I. BIPA Was Enacted To Protect Sensitive, Immutable Personal Information.

11. Following the 2007 bankruptcy of a company specializing in the collection and use of biometric information, which risked the sale or transfer of millions of fingerprints records to the

higher bidder, the Illinois Legislature enacted BIPA to regulate the capture, collection, use, and retention of biometric information by private entities.

12. The Illinois Legislature recognized that the sensitivity of biometric information was in a class of its own: "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and cannot be changed and, therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5. The risk is compounded when, as in the workplace context, a person's biometric information is also associated with his/her Social Security number and potentially other relevant financial information or personal identifiable information. The gravity of the unresolvable problems created in the event of a data breach is so severe that the unlawful collection of such information constitutes actual harm.

13. To effectuate a person's substantive privacy interest in their unique immutable biometric information, BIPA provides that a private entity may not obtain and/or possess an individual's biometrics unless it first:

(1) informs the person whose biometrics are to be collected in writing that biometric identifiers or biometric information will be collected or stored;(2)

(2) informs the person whose biometrics are to be collected in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored, and used;

(3) obtains a written release from the person whose biometrics are to be collected allowing the capture and collection of their biometric identifiers or biometric information; and

(4) publishes a publicly available retention schedule and guidelines for permanently destroying biometric identifiers and biometric information.

740 ILCS 14/15(a).

14. BIPA recognizes that without notice and consent, persons are unaware of the nature and extent of the sensitive personal information companies collect from them and use to the companies' benefit. BIPA acknowledges person's substantive privacy right in biometric information and protects such right from encroachment by private companies. Several federal courts have agreed.

15. BIPA broadly defines the biometrics to which it applies. Under the Act, a "biometric identifier" is any personal feature that is unique to an individual and includes fingerprints, facial scans, iris scans, palm scans, and DNA, among others. "Biometric information" is any information captured, converted, stored, or shared based on a person's biometric identifier which is used to identify an individual. 740 ILCS 14/10.

16. The enactment of BIPA was prescient. Today, many businesses and financial institutions have incorporated the use of biometrics into their consumer products, including such ubiquitous consumer products as checking accounts and cell phones. Moreover, the usage of biometrics has been incorporated into the labor and employment side of commerce for security and/or timekeeping purposes, as is the case here.

17. As the recent Equifax Data Breach and others have made clear, electronically stored information ("ESI") is notoriously difficult to protect and its dissemination can have disastrous consequences. The inherent difficulty in protecting ESI, combined with the uniquely irreplaceable

nature of biometric information, means that the privacy risks associated with a person's biometrics are unparalleled. Such information is far more sensitive than a Social Security number, passport, birth certificate, or similar sensitive personal information.

II. A Private Right Of Action Exists Pursuant To BIPA Against Any Entity That Captures, Collects, Stores, Or Uses Biometric Information Without Providing Notice And Obtaining Written Consent.

18. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, and use biometrics and creates a private right of action for lack of compliance.

19. At the time the BIPA was passed in 2008, another data privacy statute, the Personal Information Protection Act, 815 ILCS § 530 *et seq*. ("PIPA"), had been law in Illinois since 2006. PIPA provides a private right of action if a company possessing an individual's unique biometric data (the same data regulated by the BIPA) suffers a data security breach and fails to give affected consumers proper notice of such a breach. Further, numerous state and federal statutes, including the Illinois Consumer Fraud Act, also provide consumers a remedy in the event of an actual breach.

20. Because it believed PIPA provided insufficient protection to individuals regarding their highly sensitive biometrics, the Illinois legislature passed BIPA to expand the law to cover not only data breach cases, but also to regulate the initial collection, use, storage, and dissemination of such biometrics and the publication of information relating to same.

21. BIPA is narrowly tailored with provisions that do not place an absolute bar on the collection, capture, or dissemination of biometrics. For companies wishing to comply with BIPA, such compliance is straightforward. The necessary disclosures and a written release can be easily achieved through a single, signed sheet of paper. BIPA's requirements simply bestow on consumers

a right to privacy in their biometrics and a right to make an informed decision when electing to provide or withhold their most sensitive information and on what terms.

III. SNA Has Failed To Comply With BIPA By Subjecting Employees To A Biometric Timekeeping System Without providing Notice Or Obtaining Consent, And By Sharing That Biometric Information With Third Parties Without Consent.

22. Most businesses track workers' time using traditional method that do not collect or capture workers' biometric information.

23. Such methods can be less profitable as they cannot guarantee: (a) that mistakes are not made with respect to recording employee time; or (b) that time records are not falsified.

24. Biometric timekeeping mechanisms, on the other hand, better ensure the accuracy of employee time records because they require a person's unique, immutable biometric characteristics. As such, biometric timekeeping mechanisms can save companies significant amounts of money.

25. Because of the cost-savings, SNA elected to implement a biometric time-keeping program in lieu of less invasive—but also less profitable—timekeeping mechanisms.

26. Under SNA's timekeeping method, SNA's employees are required to provide their biometric information—namely, their fingerprints—to SNA as a condition of their employment. SNA's employees must then scan their fingers to "clock-in" and "clock-out" of work every day. Accordingly, as a part of SNA's timekeeping system, SNA captures, collects, stores, and uses its workers' fingerprints to identify them in the future for timekeeping and payroll purposes.

27. In addition, on information and belief, SNA has disseminated Plaintiffs' biometrics to payroll processors and other vendors, who store and use such information on each successive occasion it is provided by SNA and the biometric timekeeping system.

28. A worker's fingerprint scan is a distinctive identifier and constitutes a biometric identifier and biometric information under BIPA.

29. Prior to taking Plaintiffs' biometrics, SNA did not inform Plaintiffs in writing that their biometrics were being collected, stored, used, or disseminated, or publish any policy specifically about the collection, retention, use, deletion, or dissemination of biometrics. SNA did not seek, and Plaintiffs never provided, any written consent relating to the collection, use, storage, or dissemination of his biometrics.

30. Prior to taking Plaintiffs' biometrics, SNA did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.

31. Additionally, SNA did not obtain consent from Plaintiffs for any dissemination of their biometrics to third parties. Thus, SNA has violated the BIPA on each occasion it disseminates such biometrics to third parties.

32. SNA still retains its employees' biometric information. Such retention is an unlawful and continuing infringement of employees' right to privacy in their biometric identifiers and biometric information.

33. To date, SNA has never provided written notice, obtained written consent, or published the appropriate retention schedules and policies, as required by BIPA.

34. Defendant's conduct is particularly unsettling considering the economic benefit and fraud-prevention it obtains from its biometric timekeeping system, while wholly avoiding any costs associated with implementing such systems in compliance with the law. This cognizable benefit is not only to the detriment of its workers, but also to its law-abiding competitors who comply with BIPA.

35. Furthermore, Defendant's unlawful actions expose workers to serious and irreversible privacy risks—risks that BIPA was designed to avoid—including the ever-present risk of

a data breach of Defendant's systems exposing its employees' biometrics to hackers and other wrongdoers worldwide.

36. The risk to workers as a result of Defendant's actions is compounded when, as here, workers' biometric information is associated with his/her Social Security number and potentially other relevant financial information. The gravity of the unresolvable problems created in the event of a biometric data breach is so severe that the unlawful collection and/or dissemination of such information constitutes actual harm.

37. As the Illinois legislature acknowledged in enacting BIPA, persons like Plaintiffs should not have to wait until their immutable personal characteristics are stolen by criminals to have a right to pursue a claim to protect their privacy interests.

IV. Defendant's BIPA Violations Have Caused Quantifiable Injury.

38. Persons suffer informational injury when personal information about them is illegally obtained or misused, as is the case when a company violates BIPA.

39. The Illinois Legislature quantified damages for BIPA violations by expressly providing for "liquidated damages" as compensation under the Act.

40. In addition to the quantifiable injury that results when privacy expectations such as those protected by BIPA are violated, unwanted invasions of privacy also result in increased risk of harm to victims.

41. Importantly, the injury from unwanted capture, collection, storage, and use—as well as the risk of further injury posed by such actions—is greater when the information affected is highly sensitive, immutable personal information such as biometrics.

42. When biometric data is compromised, issues stemming from identity theft may be unresolvable.

43. Even the U.S. Office of Personnel Management suffered a data breach which resulted in the theft of more than 5 million employees' fingerprints by agents of a foreign state. In response, the federal government encouraged victims to obtain biometric identity theft protection services to prevent unauthorized use of their biometrics.

44. In short, the harm to persons whose rights under BIPA have been violated is recognized, concrete, and quantifiable.

V. Defendant Has Repeatedly Violated Plaintiffs' BIPA Rights.

45. During the relevant time period, Plaintiffs worked for SNA at a warehouse located at 14 Gateway Commerce Center Dr. W, Edwardsville, Illinois, 62025, which was used and possessed by Defendant.

46. Plaintiffs were required to provide their biometrics, in the form of fingerprints, to Defendant in order to work at Defendant's facility.

47. After Plaintiffs' biometrics were initially captured and collected, Defendant required them to scan their biometrics using biometric timekeeping devices each time they needed to "clock-in" and "clock-out" of work. Defendant's system ensures that Plaintiffs could only verify their own attendance and timeliness through the use of biometrics.

48. On information and belief, Defendant then disseminated Plaintiffs' biometrics to payroll processors and other vendors, who store and use such information on each successive occasion it is provided by Defendant and the biometric timekeeping system.

49. Prior to taking Plaintiffs' biometrics, Defendant did not inform Plaintiffs in writing that their biometrics were being collected, stored, used, or disseminated, or publish any policy specifically about the collection, retention, use, deletion, or dissemination of biometrics. Defendant did not seek, and Plaintiffs never provided, any written consent relating to the collection, use, storage, or dissemination of their biometrics.

50. Prior to taking Plaintiffs' biometrics, Defendant did not make publicly available any written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics.

51. Additionally, Defendant did not obtain consent from Plaintiffs for any dissemination of their biometrics to third parties.

52. Based on the foregoing, SNA violated Plaintiffs' BIPA rights: (a) when it originally captured and/or used Plaintiffs' biometrics; (b) on each occasion it required Plaintiffs to scan their fingerprints through the biometric timekeeping device; and (b) on each occasion SNA transmitted such biometrics to a third party, to the extent SNA uses third party vendors to operate its biometric program in conformance with biometric industry practice.

53. To this day, Plaintiffs are unaware of the status of their biometrics taken by Defendant. SNA has not informed Plaintiffs whether it still retains their biometrics, and if it does, for how long it intends to retain such information without their consent.

54. At the time Plaintiffs' biometrics were captured, SNA did not have a publicly available policy of informing its workers, including Plaintiffs, of what happens to their biometrics after they are captured, whether the information is disseminated to a third party and, if so, which third party, and what would happen to the information if an individual discontinues working for SNA, if the facility were to close, or if SNA were to be acquired, sold, or file for bankruptcy.

55. Plaintiffs have suffered pecuniary damages in the form of lost wages, diminution in the unique identifying value of their biometric identifiers and/or biometric information, and other costs associated with identity protection. Plaintiffs would not have agreed to work for Defendant, at least not without additional compensation, had they been informed pursuant to BIPA of the nature of Defendant's timekeeping system.

56. Furthermore, Plaintiffs' biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendant's repeated use of Plaintiffs' biometrics does and will continue to confer a benefit on Defendant for which Plaintiffs were not sufficiently compensated.

57. Plaintiffs experience mental anguish and injury when they think about the status of their biometrics and who has, or could have, access to such private information; what would happen to their biometrics if Defendant or their vendors went bankrupt or otherwise sold its assets; whether Defendant will ever delete their biometric information; what would happen if Defendant or its vendors were to experience a data breach; and how any such breach would result in irreparable harm to their identity. This harm is even more acute because an individual with access to Plaintiffs' biometrics could potentially access other financial accounts or health records which may currently, or at some time in the future, be secured through their biometrics.

58. Plaintiffs and other members of the class have continuously been exposed to substantial and irreversible loss of privacy by Defendant's retention of their biometric information without their consent.

59. By failing to comply with BIPA, Defendant has violated Plaintiffs' substantive state rights to biometric information privacy as well as the common law.

CLASS ALLEGATIONS

60. Plaintiffs bring this action on behalf of themselves and similarly situated individuals pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seeks to represent a Class defined as follows:

> All individuals whose biometrics were captured, collected, obtained, stored, used, transmitted, or disseminated by or on behalf of SNA within the state of Illinois at any time within the applicable limitations period.

61. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant; and any immediate family member of such officers or directors.

62. Upon information and belief, there are at least hundreds of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiffs, the members can be easily identified through SNA's personnel records.

63. Plaintiffs' claims are typical of the claims of the members of the Class they seek to represent, because the factual and legal bases of Defendant's liability to Plaintiffs and the other members are the same, and because Defendant's conduct has resulted in similar injuries to Plaintiffs and to the Class. As alleged herein, Plaintiffs and the Class have all suffered damages as a result of Defendant's BIPA violations and common law transgressions.

64. There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant captured, collected, stored, used, transmitted and/or disseminated the biometrics of the Class members;

b. Whether Defendant made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics, as required by BIPA;

c. Whether Defendant obtained a written release from the Class members before capturing, collecting, or otherwise obtaining workers' biometrics, as required by BIPA;

d. Whether Defendant provided a written disclosure to workers that explains the specific purposes, and the length of time, for which their biometrics were being collected, stored and used before taking their biometrics, as required by BIPA;

e. Whether Defendant's conduct violates BIPA;

f. Whether Defendant's conduct is fraudulent;

g. Whether Defendant's conduct is negligent;

h. Whether Defendant's conduct regarding the biometrics falls within the scope of an express, implied, or implied-in-fact agreement;

i. Whether Defendant's conduct constitutes an invasion of privacy;

j. Whether Defendant's violations of BIPA are willful or reckless; and

k. Whether Plaintiffs and the Class are entitled to damages and injunctive relief.

65. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitively expensive and would thus have no effective remedy. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants and promotes consistency and efficiency of adjudication.

66. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Class they seek to represent. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

67. Defendant has acted and failed to act on grounds generally applicable to the Plaintiffs and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

COUNT I
Violations Of The Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*
(On behalf of Plaintiffs and the Class and against Defendant)

68. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

69. BIPA makes it unlawful for private entities to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being captured, collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . ." 740 ILCS 14/15(b).

70. Illinois' BIPA also requires that private entities in possession of biometric identifiers and/or biometric information establish and maintain a publicly available retention policy. Entities which possess biometric identifiers or information must (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric information (entities may not retain biometric information longer than three years after the last interaction with the individual); and (ii) must adhere to the publicly posted retention and deletion schedule. 740 ILCS 14/15(a).

71. SNA is a "private entity" as that term is defined under BIPA. 740 ILCS 14/10.

72. Plaintiffs and the Class had their "biometric identifiers" collected, captured, received, disseminated, or otherwise obtained and/or used by Defendant. Plaintiffs and the Class' "biometric identifiers" were also utilized to identify them, and therefore constitute "biometric information" as defined by the BIPA. 740 ILCS14/10.

73. Each instance when Plaintiffs and the Class scanned their biometrics into Defendant's devices, Defendant captured, collected, stored, disseminated and/or used such biometrics without valid consent and without complying with the BIPA.

74. Plaintiffs and the Class have been aggrieved by Defendant's failures to adhere to the following BIPA requirements, with each such failure constituting a separate and distinct violation of BIPA:

a. Defendant failed to inform Plaintiffs and the members of the Class in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);

b. Defendant failed to inform Plaintiffs and the Class in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

c. Defendant failed to inform Plaintiffs and the Class in writing the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);

d. Defendant failed to obtain a written release, as required by 740 ILCS 14/15(b)(3);

e. Defendant failed to provide a publicly available retention schedule detailing the length of time the biometrics are stored and/or guidelines for

permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a); and

f. Defendant failed to obtain informed consent to disclose or disseminate the Class' biometrics, as required by 740 ILCS 14/15(d)(1).

75. By capturing, collecting, storing, using, and disseminating Plaintiffs' and the Class' biometrics as described herein, Defendant denied Plaintiffs and the Class their right to statutorily-required information and violated their respective rights to biometric information privacy, as set forth in the BIPA.

76. Had Defendant informed Plaintiffs that they were not being provided with the required information regarding their biometrics and the biometric timekeeping program as required by law, they would not have worked with Defendant, or he at least would have sought additional compensation.

77. Further, had Defendant provided Plaintiffs with all required disclosures, they would have been able to make an informed decision on whether to accept the offered rate of pay, whether to request accommodations related to participation in the biometric program, including whether to condition their work on being provided an alternative which did not depend on the provision of their sensitive biometric information.

78. BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of the BIPA and, alternatively, damages of $1,000 for each negligent violation of the BIPA. 740 ILCS 14/20(1).

79. Defendant's violations of the BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with BIPA.

COUNT II
Breach of Express Contract
(On behalf of Plaintiffs and the Class and against Defendant)

80. Plaintiffs hereby incorporate the foregoing allegations as if fully set forth herein.

81. Plaintiffs and the Class members entered into express agreements with SNA to provide logistical services for Defendant.

82. Plaintiffs and the Class members agreed to work for SNA in exchange for, and with the understanding that they would receive, a legally compliant work environment that adheres to SNA's own Rules and Regulations pertaining to employees.

83. These agreements were subject to implied covenants of good faith and fair dealing because Defendant had broad discretion in how to perform their duties and obligations. Defendant had virtually sole and exclusive discretion as to the work environment of Plaintiffs and Class members.

84. Plaintiffs and the Class performed all conditions, covenants, obligations, and promises owed to Defendant, including working when required and providing SNA their sensitive and confidential biometrics.

85. SNA, however, breached its agreements with Plaintiffs and the Class and failed to abide by the covenant of good faith and fair dealing.

86. As a result of Defendant's breaches of contract and the covenant of good faith and fair dealing, Plaintiffs and the Class members did not receive the full benefit of their bargain and therefore sustained actual damages for breach of contract.

87. Plaintiffs and the Class have also suffered actual damages resulting from the dissemination and exposure of their biometrics to third parties and remain at risk of suffering additional damages in the future.

88. Plaintiffs and the Class have also suffered actual damages resulting from their attempts to ameliorate the effect of the breach.

COUNT III

Breach of Express Contract Implied in Fact (in the alternative to Count II)
(On behalf of Plaintiffs and the Class and against Defendant)

89. Plaintiffs hereby incorporate paragraphs 1-80 as if fully set forth herein.

90. Plaintiffs and the Class members entered into agreements with Defendant to provide logistical services for Defendant. These agreements were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations.

91. An express contract implied-in-fact was created at the time Defendant required Plaintiffs to provide their biometrics whereby Plaintiffs agreed to provide such biometrics in exchange for, and with the understanding that they would receive, a legally-compliant work environment that prevented the unauthorized collection, use, storage, and/or dissemination of their biometrics.

92. An express contract implied-in-fact was also created at the time Defendant authorized Plaintiffs and the Class to work at their facilities whereby Plaintiffs and the Class agreed to work in exchange for, and with the understanding that they would receive, a legally-compliant work environment that prevented the unauthorized collection, use, storage, and/or dissemination of his biometrics.

93. Defendant breached their implied contracts with Plaintiffs and the Class by taking, storing, using, and disseminating to third parties Plaintiffs' and Class members' biometric information without notice or obtaining consent.

94. Furthermore, Defendant had sole and broad discretion in how to perform their obligation to provide a legally compliant workplace. Thus, Defendant also breached the implied duty of good faith and fair dealing by unfairly withholding information about the biometric program, information that was solely in Defendant's possession and control, despite requiring Plaintiffs to participate in the same.

95. Plaintiffs and the Class performed all conditions, covenants, obligations, and promises owed to Defendant, including working when required and providing Defendant their sensitive and confidential biometrics.

96. As a result of Defendant's breaches of contract and the covenant of good faith and fair dealing, Plaintiffs and the Class members did not receive the full benefit of their bargain and sustained actual damages.

97. Plaintiffs and the Class have also suffered actual damages resulting from the dissemination and exposure of their biometrics to third parties and remain at risk of suffering additional damages in the future.

98. Plaintiffs and the Class have also suffered actual damages resulting from their attempts to ameliorate the effect of the breach.

COUNT IV
Unjust Enrichment (in the alternative to Counts II & III)
(On behalf of Plaintiffs and the Class and against Defendant)

99. Plaintiffs incorporate paragraphs 1-80 above as if fully restated herein.

100. Plaintiffs bring this Count in the alternative to Counts II and III above, to the extent the finder of fact finds that there was no valid contract between Plaintiffs and Defendant.

101. By requiring that Plaintiffs and Class members provide their biometric identifiers and/or biometric information and participate in Defendant's biometric timekeeping system,

Defendant retained a benefit in the form of cost savings, increased profit, and/or increased worker productivity (achieved through eliminating timekeeping mistakes).

102. Defendant's benefit occurred to the detriment of Plaintiffs and Class members in that Plaintiffs' and Class members' substantive privacy rights were violated in the process. Such privacy rights were violated in that: (a) Plaintiffs' and Class members' biometric identifiers and/or biometric information were/was captured, collected, stored, used, and/or disseminated without their knowledge, notice, or written consent and without being provided a plan for the treatment of such information; and (b) Plaintiffs and Class members were unjustly exposed to greater risk of injury as a result of Defendant's practices with respect to their biometrics.

103. Defendant's retention of the foregoing cost-savings and profits to the detriment of Plaintiffs and Class members violates the fundamental principles of justice, equity, and good conscience.

104. Accordingly, Defendant has been unjustly enriched at Plaintiffs' and the Class members' expense, in the amount of Defendant's profits and cost-savings, among other damages, in an amount to be proven at trial.

COUNT V
Intrusion Upon Seclusion
(On behalf of Plaintiffs and the Class and against Defendant)

105. Plaintiffs hereby incorporates paragraphs 1-80 as if fully set forth herein.

106. Defendant has intentionally and unlawfully intruded upon Plaintiffs' and the Class's biometric information and data derived therefrom.

107. Such biometrics, as contemplated by the Illinois Legislature in its implementation of BIPA, constitute private affairs and concerns.

108. Thus, Defendant has unlawfully intruded upon Plaintiffs' and the Class's private affairs by failing to inform them of the purpose and length of term for which they intended to retain and use the biometrics, despite the fact that such disclosures are required by law.

109. On information and belief, Defendant has also intentionally and unlawfully intruded upon Plaintiffs' and the Class's private affairs and concerns by disseminating their biometrics to third parties, such as payroll vendors or timekeeping vendors, without knowledge and consent in violation of the law.

110. Plaintiffs and the Class had a reasonable expectation that any entity seeking to collect their biometrics, and certainly their employers, supervisors, and principals, would be doing so legally.

111. A reasonable person would find Defendant's intrusions highly offensive and objectionable, and Plaintiffs and the Class did find, and continue to find, Defendant's conduct to be both highly offensive and objectionable.

112. These repeated intrusions caused damages to Plaintiffs and the Class members in the form of, among other things, mental anguish and pecuniary harms.

COUNT VI
Conversion
(On behalf of Plaintiffs and the Class and against Defendant)

113. Plaintiffs hereby incorporate paragraphs 1-80 as if fully set forth herein.

114. Plaintiffs and Class members have a right to exclusive possession of their biometric information.

115. Plaintiffs and Class members have a right to absolute and immediate possession of their biometric information from Defendant in particular.

116. Nonetheless, Defendant wrongfully and without authorization assumed control, dominion, and/or ownership over Plaintiffs' biometric information by capturing, collecting, storing, and/or using it as a part of Defendant's timekeeping and payroll practices.

117. Any demand by Plaintiffs and Class members for immediate possession of their biometric information from Defendant would have been futile. In any event, Defendant has sold, disposed of, and/or fundamentally changed the biometric information at issue by capturing, collecting, storing, and/or disseminating it without Plaintiffs' and Class members' permission.

118. As a direct and proximate result of Defendant's actions, Plaintiffs and Class members have been damaged in an amount to be determined at trial.

119. Accordingly, with respect to Count VI, Plaintiffs, on behalf of themselves and the proposed Class, pray for an award of actual and compensatory damages in an amount to be determined at trial.

COUNT VII
Fraudulent Concealment
(On behalf of Plaintiffs and the Class and against Defendant)

120. Plaintiffs hereby incorporate paragraphs 1-80 as if fully set forth herein.

121. Defendant intentionally concealed and/or omitted the nature and extent of its capture, collection, storage, and/or use of Plaintiffs' and Class members' biometric information in order to induce Plaintiffs and Class members to provide such biometric information to Defendant. Such concealed information was material to Plaintiffs and Class members as it would be to any reasonable person in deciding whether to provide their biometric information to a third party.

122. Defendant's concealment and/or omission was intended to induce the belief of Plaintiffs and Class members that: (a) they were not providing to Defendant immutable personal information; (b) Defendant was not capturing, collecting, storing, and/or using their immutable

personal information; and/or (c) that they were not exposing their immutable personal information to dissemination to third parties and/or the risk of theft.

123. Because Defendant were Plaintiffs' and Class members' employer and/or because of Defendant's statutory duties under BIPA, Defendant had a duty to disclose to Plaintiffs and Class members the nature and extent of the biometrics Defendant collected, how such biometrics would be used and/or disseminated, and the risks therefrom.

124. Plaintiffs and Class members relied upon Defendant's silence as a representation that: (a) they were not providing to Defendant immutable personal information; (b) Defendant were not capturing, collecting, storing, and/or using their immutable personal information; and/or (c) that they were not exposing their immutable personal information to dissemination to third parties and/or the risk of theft. In the alternative, Plaintiffs and Class members could not have discovered such facts through reasonable inquiry or inspection or were prevented from making such a reasonable inquiry or inspection because Defendant maintained total control over information relating to its timekeeping program and its collection, capture, storage, and/or use of biometric information.

125. Had Plaintiffs and Class members been aware of such material information concealed and/or omitted by Defendant, they would not have accepted or continued employment, or at least would not have accepted or continued employment without additional compensation.

126. As such, Plaintiffs and Class members were damaged by their reliance on Defendant's fraudulent concealment and/or omission in an amount to be proved at trial.

COUNT VIII
Negligence (in the alternative to Count VII)
(On behalf of Plaintiffs and the Class and against Defendant)

127. Plaintiffs hereby incorporate paragraphs 1-80 as if fully set forth herein.

128. To the extent that a finder of fact concludes that Defendant did not intentionally withhold information from Plaintiffs and the Class relating to its biometric timekeeping program, Defendant was nonetheless careless and negligent in their failure to act reasonably with regards to the biometric program.

129. As more fully alleged above, special relationships existed between Plaintiffs and the Class and Defendant which gave rise to various duties and obligations concerning the biometric timekeeping and biometric data at issue because Defendant had full control over such biometric program, policies, and procedures relative to Plaintiffs' limited knowledge and power.

130. Indeed, Defendant's position relative to Plaintiffs in terms of access to information regarding the workplace, and their conduct in handling Plaintiffs' biometrics, gave rise to a duty for Defendant to act reasonably under the circumstances.

131. Defendant knew, or should have known, of the risks inherent in collecting, storing, using, and disseminating the biometrics of their workers and owed duties of reasonable care to Plaintiffs and the Class whose biometrics were obtained through their workplace relationship with Defendant.

132. Defendant knew or should have known that their agents were engaging in conduct that involved handling and dealing in the sensitive biometric data of employees and in so doing explicitly undertook a duty of care with respect to such data. Nonetheless, Defendant was careless and negligent in failing to ensure they provided compliant working conditions and met the applicable standard of care for the obtaining and handling of biometric data.

133. Defendant breached its duties to Plaintiffs and the Class with regards to biometric privacy by, among other things, failing to implement a BIPA-compliant biometric system with reasonable data security policies.

134. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class have suffered pecuniary and non-pecuniary injury, including lost wages and diminution in the value of their biometrics caused by Defendant's exposure of such information to third-parties.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully request that this Court enter an Order:

a. Certifying the Class as defined above, appointing Plaintiffs as class representatives and the undersigned as class counsel;

b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;

c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with the BIPA requirements for the capture, collection, storage, use, and dissemination of biometric identifiers and biometric information and to destroy all biometric information of Plaintiffs and of Class members in Defendants' possession and illegally obtained;

d. Awarding statutory damages of $5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);

e. Awarding statutory damages of $1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);

f. Awarding monetary damages and equitable relief for Defendant's breach of contract, negligence, unjust enrichment, intrusion upon seclusion, conversion, and fraud in an amount to be determined at trial, as well as punitive damages for Defendant's fraudulent conduct;

g. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3) as well as Fed. R. Civ. P. 23;

h. Awarding pre- and post-judgment interest, as allowable by law; and

i. Awarding such further and other relief as the Court deems just and equitable.

Respectfully submitted,

By: /s/ David Cates
David Cates #6289198
Chad M. Mooney #6311237
CATES MAHONEY, LLC
216 West Pointe Drive, Suite A
Swansea, IL 62226
Telephone: 618-277-3644
Facsimile: 618-277-7882
E-mail:dcates@cateslaw.com
cmooney@cateslaw.com

Counsel for Plaintiffs and Putative Class